Google Cloud

Threat Detection, Investigation, and Response in the Cloud

Anton Chuvakin and Timothy Peacock with Dan Kaplan

Office of the CISO

Table of Contents

Introduction and why is the cloud different?

Chapter 1

The pace at which businesses are migrating to the cloud remains rapid. Cloud adoption has been growing at tremendous rates because of the scalability, cost, and efficiency benefits of the cloud, and then the pandemic occurred. The Covid crisis pushed business migration firmly into overdrive as organizations frantically raced to satisfy the digital demand of a suddenly all-remote workforce.

Yet even as employees return to the office, the rate of cloud transition has not yielded. The overwhelming majority of companies expect to increase their cloud investment in the next 12 months, and cloud assets–including applications, hosts and containers–now outnumber physical endpoints within organizations. Given that cloud spending is only just now starting to catch up with data center outlay, we are on the brink of explosive growth.

Most security incidents now involve the cloud, according to the latest Verizon Data Breach Investigations Report. Yet organizations remain disproportionately focused on resources and efforts to protect physical, on-premises, legacy assets. Part of the reason can be chalked up to an old-school way of doing things, and the natural resistance and lag time that occurs when something new requires a dramatic shift in approach and strategy.

Organizations are facing serious security challenges. They suffer from a wide chasm in available skills and talent; an overreliance on manual processes that result in inefficiencies which then take a mental and physical toll on security teams; an unmanageable number of alerts; and ongoing visibility shortfalls. On top of those legacy problems, there's now a crucial need to adequately detect and respond to cloud-based threats. It just adds to the misery, compounded by any friction that may exist in the risk management responsibility model between cloud user and cloud provider.

> "This paper will advance the case that moving to the cloud can serve as a wedge and natural trigger to begin your security operations transformation journey."

Securing the cloud is different than protecting on-premises, but why and how specifically? Here is a sample of key reasons, some of which may bring pain while others are poised to bring possibility.

- The cloud is ephemeral and scaled: Short-lived assets predominate the cloud and are obviously easy to manage and overlook, due to their transient nature. Another problem is that assets and instances are commonly replicated in and scaled across the cloud–thus a vulnerability in one, even if has been taken offline, can ignite a ripple effect among assets that are live.
- The cloud is API driven: With the increasing cloud migration of systems and assets, businesses are using application programming interface calls as their digital "storefront" to connect with customers and partners. This has catapulted the majority of today's internet traffic to be API traffic, which has in turn invoked the interest of attackers wanting to exploit this communication path. API security is now the new frontier of application security.
- The Identity layer of the cloud is critical: Securing privileges in the public cloud, hybrid cloud and multi-cloud environments, where there live huge numbers of identities and entitlements, is much more complex than controlling access across the traditional data center perimeter. This has been evidenced by the large-scale public breaches in which adversaries gained initial footholds via identity-based attacks like phishing and credential stuffing.
- The scale of logging is much higher in the cloud: With SOC teams already overwhelmed by alerts, cloud environments are only intensifying this burden. One way to help control alert overload is by managing the log data produced by point systems, devices and applications living across the enterprise environment. But, collecting logs and making sure the right ones make it to the SIEM is no guarantee in the cloud world, largely due to uncommon log collection methods (compared to on-premises systems).
- Opportunities exist for preprocessing in the cloud: Data preprocessing takes raw data and transforms it into an understandable format. The process includes various operations, with each one aiming to help machine learning build better predictive models, including for improving attack detection in the cloud.

This paper seeks to offer an understanding of why threat detection, investigation, and response (TDIR) is different in the cloud. It also will communicate what good (and bad) can look like for all organizations (and their providers through the sharing of "fate") in the era of digital transformation, no matter what stage you have reached in your cloud and security operations maturity journey, from mom-and-pop to enterprise to MSSP.

But perhaps most impactful of all, we will advance the case that moving to the cloud can serve as a wedge and natural trigger to begin your security operations transformation journey. Adoption of cloud allows you to start that journey with the "greenfield" part of your infrastructure that is not saddled with your legacy stack. You can start doing detection and response in a new way for the new parts of your environment, and then evolve and expand this to a more traditional infrastructure.

Keep on reading, and please enjoy!

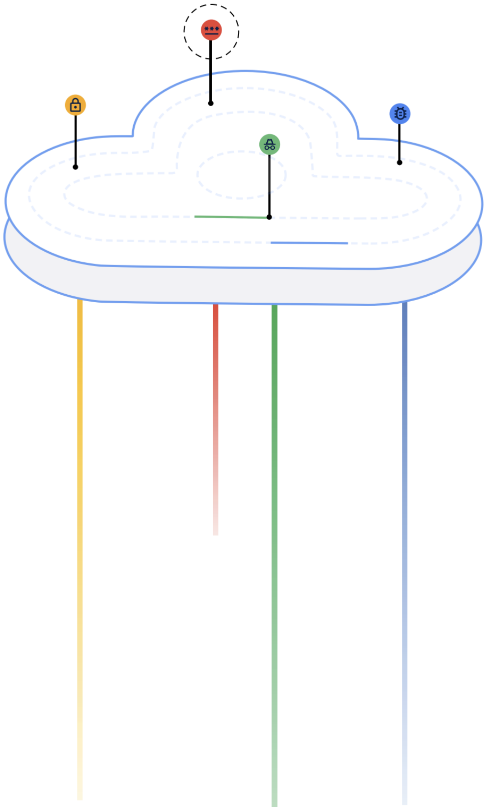
Why is TDIR different in the cloud?

Chapter 2

Here is a common scenario: You work in a SOC, and suddenly your organization embraces the public cloud. Was your team consulted about cloud migration?

Was it involved in the planning? Was it even informed in advance at all?

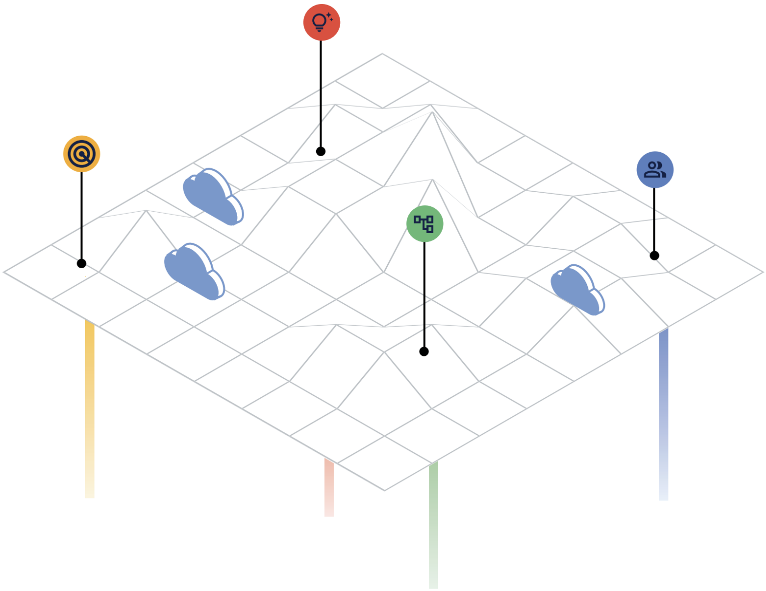
Perhaps those questions are moot by this point–in most instances, security is not a foremost consideration during the business initiative decision-making process–but that does not mean your team cannot act to reduce risk and achieve net positive security outcomes. Before you are ready to assess your personal situation and understand what you have been handed, it is pivotal to understand what makes the detecting, investigating, and responding in the cloud different.



The threat landscape is different

If you have spent any meaningful time in the security industry, the term "evolving threat landscape" likely sounds more like platitude than promise. But while cliche, it is not without merit. Indeed, as your cloud footprint rises, threats are shifting, and the attack surface which you confront daily is also changing. Not all cloud environments are created equal; for example, not all are meant to support business-critical data. However, cloud-specific threats like cloud IAM misconfigurations, overly broad cloud storage permissions, cloud bucket data leakage, remotely exploitable vulnerabilities in cloud APIS and various types of unauthorized access to cloud services should now sit squarely at the top of your watch list.

Complicating matters is that many uses of cloud services are often owned by other teams, forcing the SOC to be more collaborative than ever–another potential culture conflict. Even if you use the basic "lift and shift" approach to migrating to the cloud, your threat assessment is going to look very different. MITRE ATT&CK offers a comprehensive framework for determining which threat activities apply to public cloud computing. The Cloud Security Alliance, meanwhile, annually shares its top 11 cloud security threats.



The environment is different

Of course, not only are the threats different in the cloud, but so is the realm–aka the systems, technologies, and practices–in which you have to operate during detection, investigation, and response. While each of the major public cloud providers offers similar functionality for compute, networking and storage, providers are unique in many ways, including how security (and expertise) is delivered. For example, detecting the same threats in one public cloud requires detection rules that will be different in another public cloud. Adversaries are naturally drawn to this new paradigm, but the cloud era delivers a golden opportunity for businesses to revolutionize their offerings and provide workers with more productive ways of doing business. This includes security operations teams, who can reimagine efforts to remain resilient and protect end-users and customers.

This can be accomplished through the adoption of cloud-native tools and platforms (such as SIEM and SOAR) which allows organizations to adapt their use cases to cloud workloads and be more nimble (with less operational overhead required) in the complex effort that is TDIR. This paper will delve deeper into the security opportunities that exist for cloud adopters.

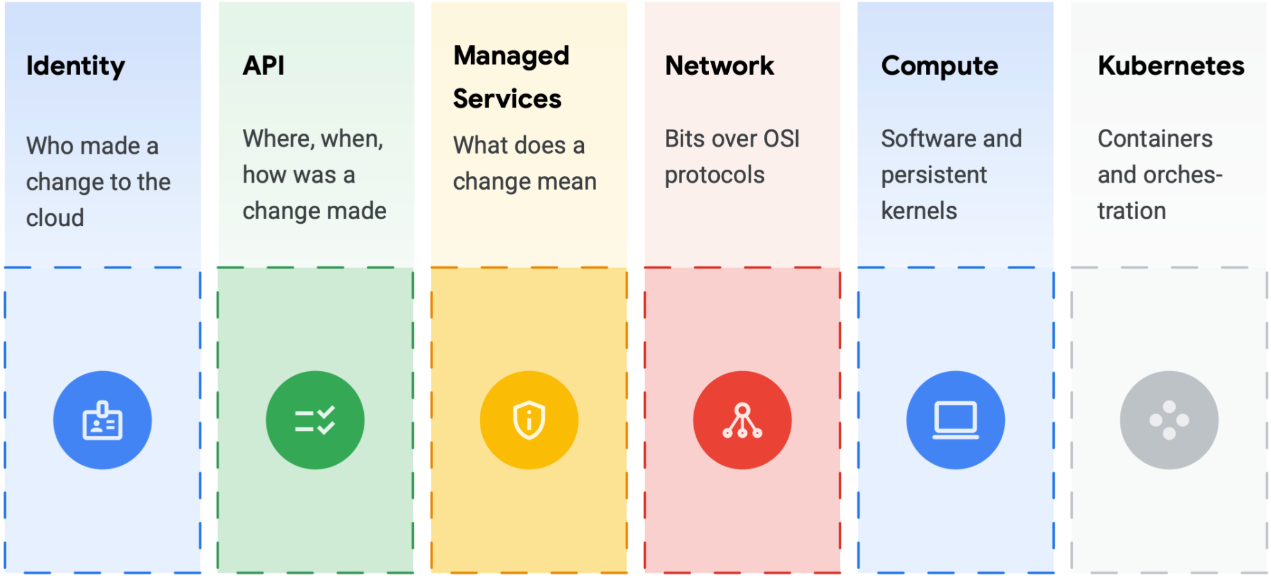
And it appears IT leaders are seizing the promise of cloud. According to technology media company Foundry's (formerly IDG) recently released ninth Cloud Computing Survey:

> *Given that the majority of (IT decision makers) have already moved or are in the process of moving a significant portion of their IT infrastructure to the cloud, it makes sense that what they want most from vendors is ongoing help managing their cloud infrastructure as a coherent, cohesive, affordable whole. Identity Who made a change to the cloud API Where, when, how was a change made Managed Services What does a change mean Network Bits over OSI protocols Compute Software and persistent kernels Kubernetes Containers and orches- tration*

Telemetry sources change and methods are different

You may assume that this is a derivative of the previous section, but that is not entirely true. Let’s look at some easy examples first. For some cloud services, and definitely for SaaS, a popular approach of using an agent such as EDR typically will not work. However, new and rich sources of telemetry may be available (cloud audit logs be- ing a prime example). Similarly, an expectation that you can sniff traffic on the perimeter, and that you even will have a perimeter may not be entirely correct. Pervasive encryption hampers layer 7 traffic analysis, while public APIs rewrite the rules on what a perimeter is. Finally, detection sources and methods are also inherently shared with the cloud provider, with some under cloud security provider control while others are predominantly under cloud user control.

This leads to several domains where you can, and should, detect, investigate, and respond to things in the cloud.



Identity

Who made a change to the cloud

API

Where, when, how was a change made

Managed Services

What does a change mean

Network

Bits over OSI protocols

Compute

Software and persistent kernels

Kubernetes

Containers and orchestration

These six domains provide cloud coverage needed (network, identity, compute, container infrastructure, etc) and some specific detec- tion mechanisms (API access logs, network traffic captures, etc).

Who does what in cloud TDIR?

Chapter 3

You are probably wondering at this point: Why is the responsibility for cloud TDIR all on us? Thankfully it is not, as public cloud providers, including GCP, offer controls

for managing these threats and making compromise more onerous on your adversaries. However, these tools experience their optimal value when organizations accept a communal burden for security.

“Shared responsibility” for security emerged from the earliest days of cloud computing as a helpful model for assigning responsibilities between cloud providers and their customers. While it made sense in the beginning, the rapidly changing security landscape means we can reimagine the shared responsibility model to better capture the full spirit of the relationship required for a true partnership to transform security in the cloud. That may sound trivial, but not having the right conceptual model in cybersecurity can lead to real-world issues. It’s time for cloud service providers to elevate their shared responsibility into a more resilient model. We call it “shared fate.”

Shared responsibility was born of questions about whether the cloud was secure, and how to best secure it. We now know that the answers to these questions are generally yes. It makes some areas of security very clear–the CSP owns physical security of servers, the security of various layers of operating systems, and other software depending on the nature of the service.

The customer typically owns the configuration, identity and access management, and the security of the application software running in the cloud. (It’s worth noting that some compliance mandates like PCI DSS include their own versions of shared responsibility models.)

But shared responsibility can sometimes set too hard of a boundary between cloud provider and customer. The result of too rigid a boundary can create, paradoxically, uncertainty as to who handles which aspects of threat detection, configuration best practices, and alerts for security violations and anomalous activities.

When security issues arise, many cloud customers question the usefulness of the shared responsibility model. Shared fate is the next evolutionary step to create closer partnership between cloud service providers and their customers so that everyone can better face current and growing security challenges–while still delivering on the promise of digital transformation.

Shared fate: What it is, why it matters

Introduced in IT operations in 2016, shared fate happens when a cloud provider and a client “work together as a team for a common goal and share a fate greater than the dollars that pass between them.” It’s a bigger-picture version of shared responsibility that encompasses it, but also transcends it.

Security shared fate is about preparing a secure landing zone for a customer, guiding them while there, being clear and transparent about the security controls they can configure, offering guardrails, and helping them with cyber insurance. Google Cloud seeks to evolve the shared responsibility to better secure our customers, and part of the challenge in adopting a shared fate mindset is that it’s less of a checklist and more of a perpetual interaction to continuously improve security.

In practical terms, shared fate’s multi-ingredient foundation is stronger than its component parts, which we’re always working on making better for your business. These features are:

• **Secure-by-default configurations.** Google Cloud’s default configurations can ensure security basics have been enabled and that users start from a high security baseline, even if some change that later.

- **Secure policy hierarchies.** Setting policy intent at one level in an application environment should automatically configure down the stack, so there's no surprises or additional toil in lower-level security settings.

- **Consistent availability of advanced security features.** Google Cloud provides advanced features to users for new products at launch, and then develops security consistency across the platform and tools.

- **Availability of security solutions.** Security solutions bridge security products and security features to cus- tomer cloud experiences, that can allow them to not just use our secure cloud, but also to use our cloud securely.

- **High assurance attestation of controls.** Google Cloud provides independent review of cloud services through compliance certifications, auditing content, regulatory compliance support, and configuration transparency.

- **Insurance partnerships.** Via the Google Cloud Risk Protection Program (currently in Preview), users can connect with insurers who offer specialized insurance for Google Cloud workloads that reduce security risk. Google works with Allianz Global Corporate and Specialty (AGCS) and Munich Re to bring a unique risk management solution to users.

Why does the future depend on shared fate?

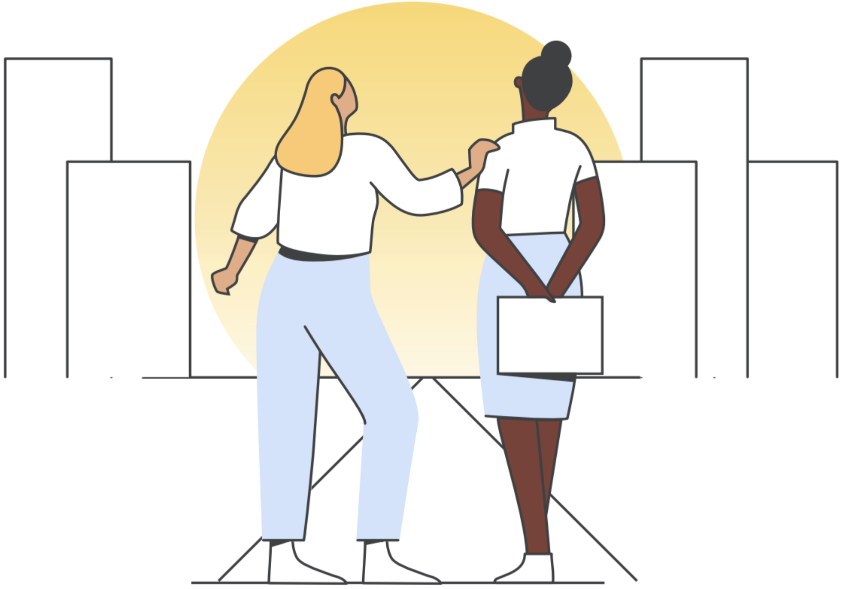
The shared fate approach can be better for cloud customers precisely because it cen- ters the customer's needs when deploying resources and applying cloud environment knowledge to security tasks. Instead of pushing responsibility to customers who may not have the expertise to properly manage it, the cloud services provider uses its considerable expertise to help the customer actually be secure in the cloud.

Given that the shared fate model originated in IT operations, it can improve defense in depth from configuration errors and defense in depth from attacks. In other words, the cloud provider can have your back, security-wise, rather than merely providing a secure platform. And by participating in the insurance ecosystem, we help bridge the gap between the technical controls in the cloud environment and risk coverage.

Shared fate does not mean "no customer responsibility" for security. No cloud provider can do the 100% of work securing each customer's use of the cloud, and the customer will continue to be ultimately accountable for their risks. There will always be a set of tasks and activities focused on security that cloud customers will need to undertake. Instead, we believe that CSPs can and should do more to build the security shared fate with customers and use their substantial cloud and security experience to help reduce risks for clients as they transition to the cloud.

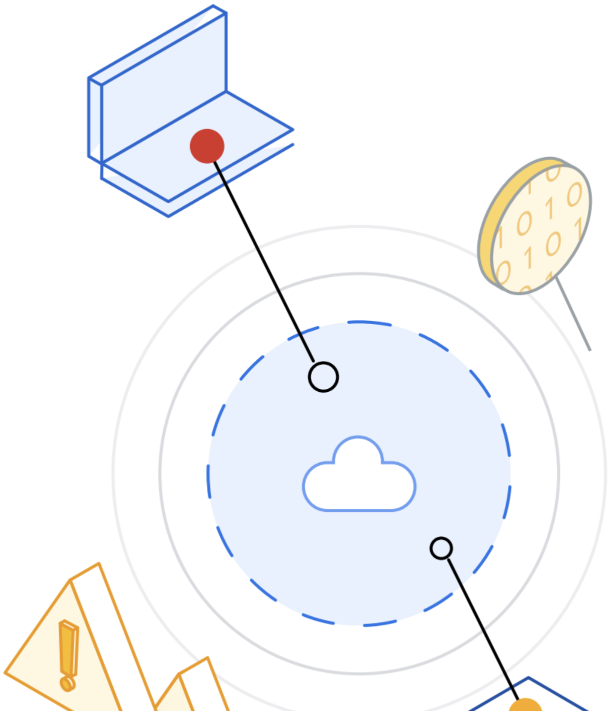
The shared fate model can more accurately represent the journey to the cloud, help- ing to manage and reduce risk while organizations and their leaders transform their business, IT, and cybersecurity for the modern era. The sooner we adopt it as standard practice, the safer we all can become.

How do you do cloud TDIR?



Introducing an integrated SecOps model

Chapter 4



We've said a lot. What does it all mean for you? Let's review.

When you move to the cloud, your threats change enough–and your IT environment changes a lot–that the purely on-premises detection technology and engi- neering approaches and tools you have relied on should not be expected to perform as adequately.

Instead, moving to cloud is a chance to rethink how you can achieve your continued on-premises goals of confidentiality, integrity, and availability with the new opportunities created by the technology and process of cloud computing.

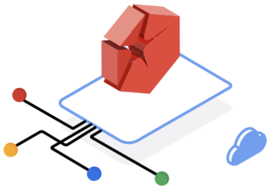
That will mean that, as a defender, you will need to at least mix and match your existing tools with newer options. One way to get started is through a security operations architecture that interoperates and integrates across the TDIR cycle, and helps you vastly reduce your time spent doing TDIR, a span of time that is directly correlated with how impactful a data security incident will be.

Here is how Google Cloud Security offers a holistic and unified approach to cloud-based threats that is mapped to three products: Security Command Center, Chronicle SIEM and Siemplify SOAR. Combined, you can receive a richer, higher-fidelity and context-aware TDIR experience, allowing you to make better and faster decisions when it matters most.

So, how does it all integrate?

01. Security Command Center Premium is Google Cloud's native risk and security tool. SCC Premium provides real-time asset, misconfiguration, and threat visibility by surfacing security issues. Its threat detection is provided as a managed service that minimizes the DevSecOps burden, while providing ever-improving visibility detection for the most damaging cloud threats. SCC helps protect your security policies, identi- ties, managed databases, compute engine instances and Kubernetes clusters.

02. The alerts and events surfaced by SCC are sent directly into Chronicle SIEM at unprecedented speed and scale to perform detailed investigation of the threats, including emerging and potentially sophisticated cloud-based risks, in near-real time. Chronicle normalizes, indexes, and correlates the security and cloud telemetry to provide instant analysis and context on malicious activity.



03. Finally, **Siemplify SOAR** steps in to streamline and automate detection and response to these alerts and events with out-of-the-box playbooks that automatically contextualize the threats, denote malicious files and close false positives. Coupled with case management and team collaboration, Siemplify SOAR also ensures fast and timely response, and will trigger remediation sequences and threat hunts across the organization.

All told, this SecOps suite offers a turn-key best-in-class detection, prioritization, investigation, and response journey for organizations like yours experiencing a classic disconnect: the generous embracing and adoption of the public cloud by the business but considerable discomfort within the security operations team about the ability to stay protected. In addition, with Google, you gain access to thought leadership, a rich partner ecosystem, and expert advice to drive SOC transformation. We wrote the defining work on Autonomic Security Operations, which drives 10x SOC improvement, and our security team and partners are here to ensure you always achieve your desired security outcomes.